International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 5, October 2018, pp. 3267~3277
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i5.pp3267-3277

An Effective Data Privacy Mechanism through Secure Session Key Exchange Model for MANET

K. Ramesh Rao[1], S.N.Tirumala Rao[2], P. Chenna Reddy[3]
[1]CSE, JNTUA, Anantapuramu (A.P), India
[2]Department of CSE, NarasaraoPeta Engineering College Narasaraopet, India
[3]Department of CSE, Director, Academic Audit, JNTUA, India

Article Info

Article history:

Received Oct 12, 2017
Revised Apr 10, 2018
Accepted Sep 22, 2018

Keyword:

Data security
MANET
Network Stability
Privacy
Session key exchange

ABSTRACT

Data privacy in the mobile ad-hoc network is a problem due to wireless medium, frequent node movement and lack of any centralized infrastructure support. In such case, it is very important to build a reliable and secure network and achieve high throughput in MANET. The reliability and security of a network depend on whether the network remains linked to different failures and malicious activities, which is the fundamental issue that needs to be focused when designing a secure routing protocol in MANET. This paper proposes an effective privacy mechanism to handle data security through a novel secure session key exchange model, which provides the node data privacy and network stability for a longer period of time and prevents abnormal behavior changes due to malicious behavior and different type of attacks in the network. The simulation results show improvement in throughput with nominal overhead and end-to-end delay in different malicious conditions against existing protocols.

Corresponding Author:

K.Ramesh Rao,
Department of CSE,
Jawaharlal Nehru Technological University,
Anantapuramu(A.P)-India.
Email: karanamramesh@yahoo.com

1. INTRODUCTION

Mobile ad hoc networks benefit greatly from wireless communications because of their infrastructure independence and the multi-hop nature of communications. However, this advantage poses a significant challenge to data security and privacy management, which affects secure data delivery in mobile ad-hoc networks because of high numbers of attacks and dynamic topology changes on wireless channels. At the same time, network stability is an integral part of reliable communication services. Since the operating range is not limited to the topology, it is likely to be intrinsically damaged. This is because it is very difficult to ensure temporary routing of this difficulty in order to preserve the "centralized policy" or "scheme" of the existing network. Various ad-hoc routing protocols[1], [2], [3], [4], [6] deal with security requirements and some of the proposals in the past have targeted high vulnerabilities in ad hoc networks. In addition to the above difficulties, the resources of MANET cause major problems in security process deployment and major constraints limitation. The protocols AODV and DSR routing are very efficient, but both are vulnerable to various types of attacks.

In the past several routing protocols have been proposed [1], [6], [7], [10], [12] that are well suited to the dynamic characteristic of ad-hoc networks. Nevertheless, these routing protocols assume security and believe that all nodes in the environment are supportive and trustworthy. This assumption is not valid. However, it is almost impossible to maintain prerequisites on a real network in view of potential node malfunctions and random failures. For example, a rogue node cannot pass control or data packets to another

node to store its resources and can initiate a denial of service (DoS) attack and interfere with normal communication procedures. Many studies have been performed to characterize various node malfunctions and to assess their impact on network performance. However, little research effort has been made to analyze how much they affect node personal information during data communication.

In this paper, we propose an effective Data Privacy Mechanism (DPM) through Secure Session Key Exchange (Sskey) Model to establish node privacy during data communication. It contributes a distinct Sskey for each data route from source and destination for the data privacy communication. It provides a secure communication method that uses "symmetric encryption" and "authentication routing" to protect messages. It protects the data with a unique, trusted encryption key that is generated using a trusted path. This has the advantage of improving QoS by minimizing high "throughput" and "end-to-end delay" in low-cost routing constraints. The objective of this paper is to secure an existing ad-hoc routing protocol, AODV [11], by extending it in an approach that non-malicious nodes can distinguish and segregate malicious nodes from the network so that it cannot interrupt the network. In this paper, to overcome these vulnerabilities problem we evaluated the existing "AODV, S-AODV [15], EAACK [9] and FACE [8]" protocols. In the Section 2, we describes related works that provide an overview of the secure routing protocol. The efficient data privacy mechanism is proposed in Section 3, Section 4discusses the privacy analysis, Section 5, presents the Results of Evaluation, and Section 6 discusses the conclusions.

2. RELATED WORKS

To ensure security and privacy of messages in routing is a primary concern in AODV routing [11]. An efficient authentication mechanism is needed to ensure a secure message exchange between the sender and the receiver. AODV configures routes as needed because of its responsive routing protocol, which provides short network overhead and utilizes a default sequence number to prevent routing loop avoidance attacks. Mainly, three forms of messages are exchanged for communication "RREQ"," RREP", and "RRER" [4]. Each node in the path broadcasts an RREQ and verifies the information accumulated in the routing table and the sender serial number of the RREQ message. If it is new request it must be updated in the routing table to prevent routing loop vulnerability attacks. In addition, many other vulnerability attacks, such as "spoofing", "denial of service", and "message tampering", are serious problems with the AODV protocol. There are many secure ad hoc routing protocols presented for mobile ad-hoc routing [7], [9], [10], [20], [21], [23] because of its high-security vulnerabilities caused due to its openness and communication environment.

Since we extend the features of AODV [11] in this work we describe its mechanism to understand its advantage in dynamic routing. It is a reactive routing protocol for mobile ad hoc networks that constitute a route on demand [26]. It utilizes sequence numbers to provide minimum network overhead and avoid a number of routing loop to perform maintenance and communication control it exchanges the standard "RREQ"," RREP", and "RRER" messages. Each node maintains an individual routing table to route data packets to the target node. But it does not secure its route data and messages which are a major cause of data loss in AODV. It needs a secure authentication mechanism to protect sender and recipient messages. During route request broadcast, every one node makes sure the sender "sequence number" of the "RREQ message" in opposition to the stored information in the routing table. For the route responses, as a substitute of scrutiny the sender "sequence number", it confirms the destination node "sequence number" and remains the routing information restructuring. All vulnerability attacks result in a routing loop or packet loss. In addition "routing messages fabrication", "spoofing" and numerous other attacks have a severe impact on the AODV protocol.

Zapat et al. [13] propose an authentication mechanism as Secure-AODV to secure intermediary nodes from the malicious and illegal spoofing identity information activity. It even discusses the securing process for "modify the number of hops count" and "route fabrication" error messages. The mechanism is an addition to the AODV protocol supported by "public key cryptography" to give routing security. It mostly ensures the integrity and reliability through digitally signed routing and controls messages. Each time a node which generates a routing message sign with a "private key"; the node receiving this information verifies and authenticates the signature using the "sender's public key". A mechanism supported by a "hash chain" is used to protect it. The larger symmetric encryption used for digital signatures produces long messages. Each time the intermediate node receives a message, it has to verify the "signature" for authentication. Using double signing mechanisms for message verification it creates higher load over the network.

S K. Dhurandher et al. [8] proposed a "Friend based Ad hoc routing using Challenges to Establish Security (FACES)" to offer secure communication in MANET routing. It defines a method for building a secure network based on a list of friends who share a list of nodes in a friend network. Every node periodically executes a process to retrieve a list of shared friends, creating a friend's node responsibility. Based on this intervallic update, malicious nodes can be easily removed from the network. This approach does not need to observe neighboring transmissions for node reliability assessment. The disadvantage of this

proposal is high "end-to-end delay" because of the computational overload and malicious behavior of the friend node, which can affect the entire friend list, communication, and network stability.

M. S. Elhadi et al. [9] proposed an "intrusion detection system" known as "Enhanced Adaptive Acknowledgment (EAACK)"for MANETs. This work mainly focuses on the "packet drop attack" which is a security threat of MANET. It tried to prevent an attacker from attempting a fake acknowledgment attack involving a digital signature. This paper proposes an effective data privacy mechanism protocol to overcome the above observations in the routing privacy of AODV and other secure routing protocol and present an evaluation comparison with "AODV", "S-AODV", "EAACK" and "FACES" secure routing protocol.

3. PROPOSED DATA PRIVACY MECHANISM

An ad-hoc routing protocol node exchanges information with neighboring regions and configures a network for routing data packets to the required destination. An "external attacker" typically introduces incorrect routing information into the route to repeating preceding routing messages or modifying applicable routing information, which ultimately breaks the network. Internal attacks can cause serious damage because the node does not meet the initial commitments. These nodes can easily alter the confined outlook of the network by sending incorrect information. In general, it is very complicated to recognize an internal intruder, as these nodes are included in the network due to their security credentials.

The proposed Data Privacy Mechanism (DPM) intend to target both internal and external type-specific attacks to provide the highest level of privacy. The DPM approach can identify and enforce the necessary precautionary measures by implementing a secure privacy mechanism for both route discovery and data routing. It utilizes a trusted third-party (TTP) certificate that consists of all the initial required keys to protect the private information from internal and external attackers.

3.1. Privacy Model

The privacy model consists of three secure process mechanisms to establish data privacy mechanism as shown in Figure 1. Here the source node initially obtained the TTP certificate to participate in the communication, later to do the data communication it builds secure route through route discovery process utilizing DP mechanism. It utilizes the discovered data route for the data routing along with the privacy maintenance.

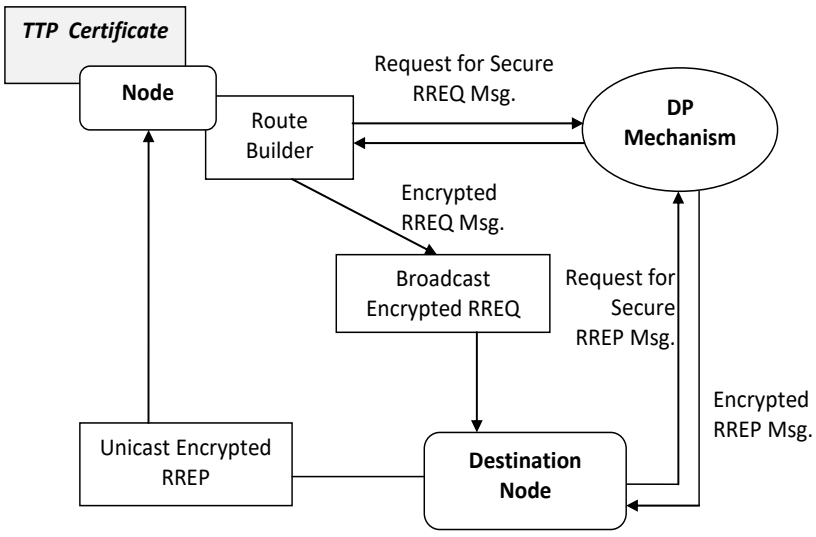

Figure 1. Data privacy model

3.2. Data Privacy Mechanism

This section discusses the privacy mechanisms as shown in Figure 1. This categorizes the mechanism as, 1). "Acquiring TTP Certificate", 2). "Secure Route Discovery Privacy" and, 3). "Secure Data Routing Privacy" for the secure data routing and achieving the quality of service.

3.2.1. Acquiring TTP Certificate

Establishing a secure communication between network nodes is the hardest part in MANET. Due to its constraints and characteristics reasons, it is challenging to utilize the predefined architectures for security. In the most secure routing protocols, the operations are related to privacy and key distribution was not properly handled. The previous secure routing protocols related to secure routing and key distribution are not the best due to computation overhead and storage. The "group key exchange" mechanism is being described in [21], which can be a simplified solution for the overhead of secure routing between the source and the target node.

The mechanism of group key distribution is based on strong keys sharing, which is an effective mechanism in the case of high mobility behavior where nodes participate and move very often. An asymmetric encryption based security associations between nodes are being discussed [18] and [19], where it issued secure certificates of each individual node in the network provided by a TTP. It is a secure and strong process, as the distribution of certificate is done at a single point. However, if the malicious nodes are already in the network, then vulnerability attack can intrude the certificate or gain a certificate loaded and can easily acquire the identification of the new node causing insecurity to the node and network stability.

In this data privacy mechanism, we distribute certificates with initial secure connections between the nodes. However, this certificate comes from a "trusted certification authority (CA)" and must be loaded on every node before connecting to the network. It is an "offline process" in which every node must present its own individuality to the "CA" to acquire the certificate. In this approach, if whichever node attempts to own an "invalid certificate", it can be easily recognized and made in accessible legally. The certificate offered by the "CA" for a node N will consist of "CA public key as CApub_key", "node address as Nadd", "public key as Npub_key" and private key as "Npvt_key". It is can be represented as shown below,

$$C_N = Enc_{CA_{pkey}} (N_{add}, N_{pub\_key}, N_{pvt\_key}, CA_{pub\_key}) \quad (1)$$

We structure that all applicable nodes in the network to get this "CN Certificate" in prior to connecting to the network.

3.2.2. Route Discovery Privacy

To perform the route discovery with privacy, we extend "AODV" [11] route discovery mechanism and integrates the privacy mechanism. The discovery process is performed in 5 steps.

Algorithm 1: *Secure Route Discovery Mechanism*

Initialization of route request RREQ by Source Node, $SN \rightarrow Start\_RREQ\ (SN_{rreq})$

Method-1: $Start\_RREQ\ (SN_{rreq})$

SN execute DH Algorithm to Generate a "Session Key" $\rightarrow SA_{SKey}$
SN create *msg* signature through $Eypt\_SAH1(Msg) \rightarrow SA_{sign}$
SN create broadcasting *msg* through $Eypt\ (Br\_Msg)_{CApub\_key} \rightarrow E_{br\_msg}$
SN create $Eypt([SA_{sign}, E_{br\_msg}, SA_{SKey}, DN_{add}, P, T_{stamp}])_{CApub\_key} \rightarrow B_{rreq}$
SN broadcast generated B_{rreq} for the intermediate nodes as, *I* in the network.

while each address of $I_i \neq DS_{add}$ **then**
  I_i execute $Dypt(B_{rreq})_{CApvt\_key} \rightarrow [SA_{sign}, E_{broad\_msg}, SA_{SKey}, DN_{add}, P, T_{stamp}]$
  I_i execute $Dypt(E_{br\_msg})_{CApvt\_key} \rightarrow Br\_Msg$
  I_i execute $Eypt\_SAH1(Br\_Msg) \rightarrow IA_{sign}$
  If $Compare\_authSign(IA_{sign}, SA_{sign}) == 1$ **then**
    If $Compare(Br\_Msg, 'RREQ') == 1$ **then**
      If $Compare\ (I_i \text{ add}, DN_{add}) == 1$ **then**
        Update $SN\ SA_{SKey}$ in destination route table $\rightarrow DR\_Table$
        $Start\_RREP\ (DN_{add});$
      Else
        I_i update its address to $P \rightarrow Update(B_{rreq}, I_i) \rightarrow NB$
        $I_i\ Eypt(NB)_{CApub\_key} \rightarrow B_{rreq}$
        I_i broadcast generated B_{rreq} in the network.
      End if
    End if
  End If
End while

Method - 2: *Start_RREP (DN_{add})*

DN execute DH Algorithm to Generate a "Session Key" → DA_{SKey}
DN create *msg* signature through *Eypt_SAH1(Msg)* → DA_{sign}
DN create reply *msg* through *Eypt (Rep_Msg)*$_{CApub\_key}$ → E_{rep_msg}
DN create *Eypt([*DA_{sign}, E_{br_msg} , DA_{SKey} , SN_{add}, *P,* T_{stamp} *])* $_{CApub\_key}$ → B_{rrep}
DN unicast B_{rrep} through the path recorded in *P* to reach *DN*.

while each address of $I_i \neq SN_{add}$ **then**
I_i execute *Dypt(*B_{rreq}*)*$_{CApvt\_key}$ → *[*DA_{sign}, E_{broad_msg} , DA_{SKey} , SN_{add}, *P,* T_{stamp} *]*
I_i execute *Dypt(*E_{br_msg}*)*$_{CApvt\_key}$ → *Br_Msg*
I_i execute *Eypt_SAH1(Br_Msg)* → IA_{sign}

If *Compare_authSign(*IA_{sign}, DA_{sign} *)* == 1 **then**
If *Compare*(*Br_Msg* , '*RREP*') = = 1 **then**
If *Compare* (I_i add, SN_{add}) == 1 **then**
Update *DN* DA_{SKey} in source route table → *SR_Table*
Else
I_i get route *P* from *Br_Msg* → *R*
I_i get next hop node from *R* → N_{hop}
I_i unicast B_{rrep} to N_{hop}
End if
End if
End If
End while

In step-1, it prepares secure RREQ packets encrypted using CApub_key, in step-2 it broadcasts the encrypted RREQ message in the network and waits for the reply from destination, in step-3, intermediate node rebroadcasts the RREQ message, in step-4, destination node creates a session key, Sskey and creates the route reply, RREP message, and finally in step-5 destination replies the secure RREP message to source. Source on receiving the RREP from destination updates the path in its routing table along with session key for that path.

Algorithm-1 provides a secure route discovery process used by DPM for route discovery. It describes the above functionality in two methods. Method-1 describe the mechanism of the RREQ broadcasting by source and functionality of intermediate nodes and method-2 describes the mechanism of destination node on arrival of RREQ and RREP to the source.

3.2.3. Data Routing Privacy

Data routing is the next process after completing the secure route discovery process by the source node. Each node in the route maintains its previous and next hop details for the data routing to the destination. Mostly source node transmits the data through the most favorable and short route based on the routing table and in the case of the AODV protocol it preserves only one path from the source to the destination. In this mechanism, we retain the feature of AODV to lower routing overhead. It secures the data packets before sending using the unique destination session key provided by the destination node. Using the destination unique session key source initially generates a secret key as SCKey. Let's consider DSKeyis the unique session key from the destination which is generated using a DH algorithm.

The data need to transmit to the destination is encrypted using the generated SCKey; as the decryption key is already available with destination it decrypts the data received efficiently. This mechanism is illustrated in Algorithm-2. Here, the functionality of the data routing is performed in two methods. Method-1 describes the steps for a secret key, SCKey generation, data encryption and data transmission, whereas Method-2 describes the steps for generating a unique secret key, SCKey using DSKey and data decryption on receiving. It also creates the secure DELV_ACK message for the reply on the successful data packet delivery.

Algorithm 2: *Secure Data Routing Mechanism*

Initialization of data transmission by Source Node, $SN \rightarrow StartDataTx(\ DN_{add}\ ,\ Seq\_No)$

Method-1: $StartDataTx(\ DN_{add}\ ,\ Seq\_No)$

SN read routing path from routing Table → *R*
SN read secure destination key → DA_{SKey}
Create distinct key for data encryption using $DA_{SKey} \rightarrow UA_{Key}$

For (*t=0, t<number_of _pkt, t++*) **loop**
Data packet to transmit → DP_t
SN create secure data packet using $UA_{Key} \rightarrow Eypt(DP_t\ ,\ UA_{Key}) \rightarrow E_D$
SN transmit the E_D to its next hop in its *R*.
while ($ACK\_Time \neq 0$) **then**
If (*Received* E_D) **then**
SN read secure destination key → SA_{SKey}
Create distinct key for data encryption using $SA_{SKey} \rightarrow UA_{Key}$
SN decrypt E_D using $UA_{Key} \rightarrow Dypt(E_D\ ,\ UA_{Key}) \rightarrow D_{msg}$
If (compare (D_{msg} ,*"DLV_ACK") == 1)* **then**
End While;
Transmit next data packet → $StartDataTx(\ DN_{add}\ ,\ Seq\_No);$
Else if ($ACK\_Time \neq 0$) **then**
Re-transmit next data packet → $StartDataTx(\ DN_{add}\ ,\ Seq\_No);$
End If
End If
End While
End For

Method2: $RecieveData(E_M, pkt\_seq\_no)$

Destination node *D* on receiving the data packets,

D gets its own Session Key → D_{SKey}
D generate unique Secret key using $D_{SKey} \rightarrow SC_{Key}$
D decrypt the data packets using $SC_{Key} \rightarrow Decrypt(E_M\ ,\ D_{SKey})$ -> D_M

D gets its Source Session Key → S_{SKey}
D generate unique Secret key using $S_{SKey} \rightarrow SC_{Key}$
D decrypt the *DELV_ACK* message using $SC_{Key} \rightarrow Decrypt(DEL\_ACK\ ,\ D_{SKey}) \rightarrow E_M$
D Sends secure acknowledge E_M back to source.

Mostly source node transmits the data through the most favorable and short route based on the routing table and in the case of the AODV protocol it preserves only one path from the source to the destination. In this mechanism, we retain the feature of AODV to lower routing overhead. It secures the data packets before sending using the unique destination session key provided by the destination node. Using the destination unique session key source initially generates a secret key as SCKey. Let's consider DSKeyis the unique session key from the destination which is generated using a DH algorithm. The data need to transmit to the destination is encrypted using the generated SCKey; as the decryption key is already available with destination it decrypts the data received efficiently. This mechanism is illustrated in Algorithm-2.

Here, the functionality of the data routing is performed in two methods. Method-1 describes the steps for a secret key, SCKey generation, data encryption and data transmission, whereas Method-2 describes

the steps for generating a unique secret key, SC_{Key} using D_{SKey} and data decryption on receiving. It also creates the secure DELV_ACK message for the reply on the successful data packet delivery.

4. PRIVACY ANALYSIS

The path discovery process must discover paths through intermediate node collaboration. The attack on a route through "Route fabrication attack" can result in changes to path message modifications. To provide a solution, to this attack DPM uses TTP public keys to encrypt messages. The "Route cache poisoning attack" incorrectly routes a node to the wrong path.This attack is handled through implementing different private keys at both the origin and destination. The malicious node does not affect the route cache, which can transmit the incorrect route, each first route request message is very secure and protected by the "private key" and the node's "public key" for the regular route message security. The "DoS" or "packet dropping" is another issue in route discovery and does not interfere with the discovery mechanism until a non-malicious node is presented in the network. To prevent this, DPM requires each contributing node to have an "ID" and a valid "TTP certificate". We investigate possible attacks [23] on route discovery and routing and countermeasures taken by DPM to protect routing in mobile ad-hoc networks [27], [28].

4.1. Attacks on Route Discovery Process

a. Message Fabrication: Route discovery procedure requires intermediate node collaboration to discover routes to the destination. Attacks on intermediate nodes can lead to modification of route messages. To prevent "message fabrication" DPM encrypts path messages symmetrically and asymmetrically and encrypts them by means of the node "public key". This new contribution gives an additional guarding against the attackers passing through the path to perform path message fabrication.
b. Cache Poisoning: This type of attack guides the node to route data to the wrong path. The DPM handles this attack with trusted keys, available at both source and target nodes. If a malicious node broadcasts an invalid route, it will not affect the "route cache". First, every route request message is protected by a trusted key and a node public key, and later it is secured utilizing the"unique secret key" that is completely independent of the normal route message.
c. DoS in Discovery Process: Denial-of-service (DoS) in path discovery or packet loss is an unreceptive malicious characteristic that does not interfere with the discovery procedure. To prevent this category of behavior, DPM makes certain that each included node need to have a valid and trusted "CA certificate".

4.2. Attacks on Data Routing Process

a. Data Packet Fabrication: During data communication, an intermediate node is able to inject a "false route" by changing the data packet to reduce throughput. The DPM handles data packet fabrication by encrypting data packets using a secret key that is unique during routing. Together the source node and the destination node generate a "unique secret key" that transmits data packets and notifies the acknowledgment messages.
b. Data Packet Dropping: Dropping data packets is a general behavior of malicious nodes that affect network QoS. The proposed DPM prevent this attack through authentication of a trusted CA certificate for each node which is a necessity for joining the network.

5. EXPERIMENTAL EVALUATION

The experimental evaluation supposes that both kind "internal" and "external" malicious nodes occur in the network. Nevertheless, it is also believed that the majority notes in the network are trusted. We utilize node "public key cryptography" to look after the network security using symmetric encryption for data transmission and messaging attacks against external and internal attacks. The simulation is made using the Glomosim Simulator which provides a scalable and configuration driven evaluation. The proposed DPM is deployed in this simulator and evaluated against the configured parameter and also compares with the result of "AODV [11], S-AODV[13], EAACK[9] and, FACES [8]".

5.1. Network Setup

This section discusses the set of parameters required for the simulation the protocol. The simulation is executed in a "Random Way Point (RWP)" model with mobility changes from "10m/s to 100 m/s". The simulation is carried out in two scenarios. Inthe first scenario communication is made without malicious node in the network, whereas in the second scenario with a 40% malicious nodes. The required parameter for the simulation is shown in Table 1.

Table 1. Simulation Parameters

Configuration	Values
Simulation Area	1200m X 1200m
CBR Rates	4 pkts/sec
Packet Size	512 bytes
Source-Destination Paris	20
Pause Time	25 sec
Mobility	RWP
Mobility Speed (m/s)	10,20,40,60,80,100

In the route discovery phase, every node is authenticated by means of CA certificate, and they all behave like normal and secure nodes. To have an impact of malicious behavior40% malicious node are configured for the data routing during simulation.

5.2. Experimental Results

5.2.1.Throughput

Throughput performance comparison is shown in Figure 2(a) and Figure 2(b). All protocols illustrate related results in comparison. In the case of "without malicious nodes, "every protocol shows similar kind of results and deteriorate with increasing mobility. But in the case of "40% malicious nodes," DPM performs better than others. This is due to effective data packet securing. The malicious node unable to decrypt the message due to its secure protection of unique secret key and which prevents unwanted fabrication and support in better throughput. The DPM show an average improvisation in the case of without malicious due to its cryptography overhead, and in the case of with malicious it shows a 25% better throughput compared to other protocols.

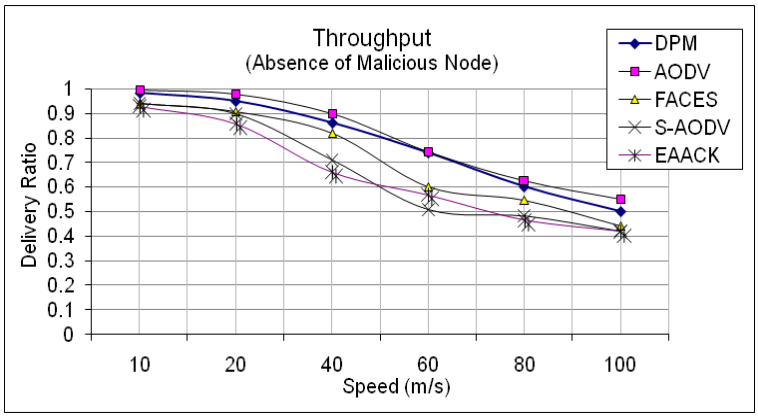

Figure 2(a). Throughput comparison without malicious nodes

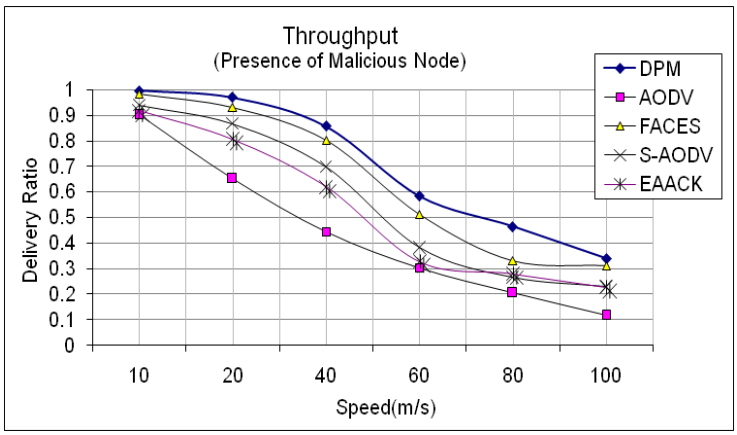

Figure. 2(b). Throughput comparison with 40% malicious nodes

5.2.2. End-to-End delay

End-to-end delay performance comparison is shown in Figure 3(a) and Figure 3(b). In the case of, without malicious node, all protocols show a similar rate of delay up to 40m/s mobility, but with increased mobility, they all attain high delay due to frequent link failure. However, in the case of with 40%, malicious DPM and FACES show less delay in comparison to other protocols, as both implement the certificate acquisition process which allows safe and secure identification of node which supports minimizing packet loss and end-to-end delay.

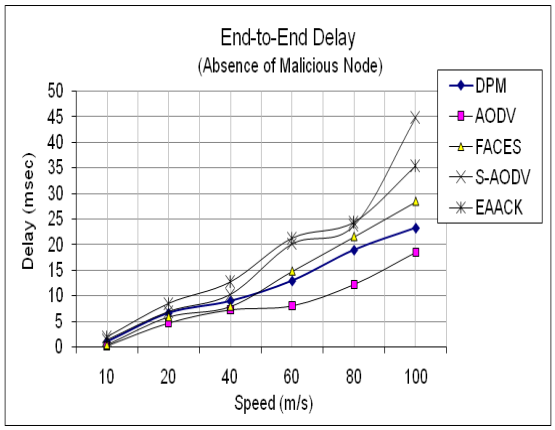

Figure 3(a). End-2-end delay comparison without malicious nodes

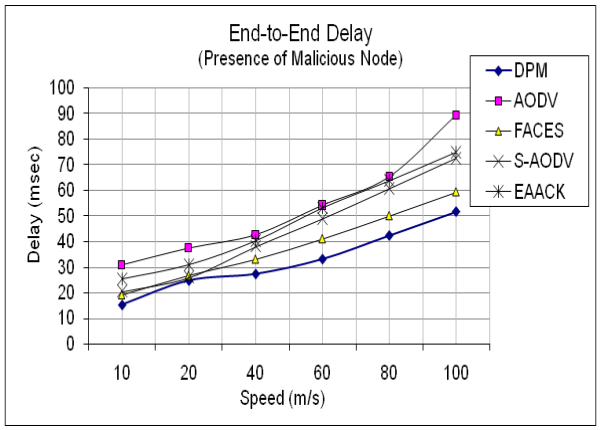

Figure 3(b). End-2-end delay comparison with 40% malicious nodes

5.2.3. Control Overhead

Control overhead performance comparison is shown in Figure 4(a) and Figure 4(b). Here, in the case of no malicious node, all protocols have similar distribution overhead as all suffer due to a link failure under high mobility conditions. In case of with 40% malicious a parallel increment of overhead is observed for all up to 60% mobility due to its security and authentication overhead, but DPM maintains the overhead low, whereas other protocols result in higher overhead.

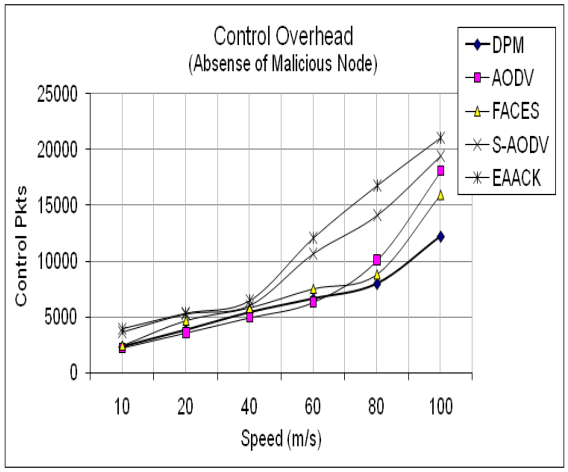

Figure 4(a). Control overhead comparison without malicious nodes

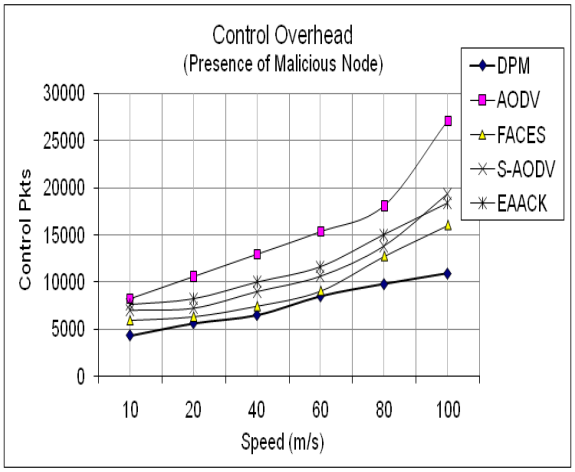

Figure 4(b). Control overhead comparison with 40% malicious nodes

6. CONCLUSION AND FUTURE WORKS

In this paper, we propose an efficient data privacy mechanism (DPM) for mobile ad-hoc networks that protects routing mechanisms from internal and external attacks. It authenticates the route discovery

mechanism by securing the control messages using public key cryptography with symmetric encryption and using unique session and secret keys to protect the data routing mechanism. Both mechanisms provide a secure and quality of service establishing the data privacy mechanism through acquiring TTP Certificate and implementing privacy for route discovery and data routing. The experimental evaluation is made with and without malicious node scenario to compute the throughput, end-to-end delay, and control overhead. The comparison result of DPM shows an average 25% satisfactory improvement in throughput, but it attains bear minimum delay higher than AODV due to its security mechanism computation and it shows an average 20% low control overhead in comparison.

REFERENCES

[1] F. A. Khana, M. Imran, H. Abbas, M. H. Durad, "A detection and prevention system against collaborative attacks in Mobile Ad hoc Networks", *Elsevier Future Generation Computer Systems*, Volume 68, Pages 416-427, 2016.

[2] M. Gharib, Z. Moradlouc, M. A. Doostaric, A. Movagharb, "Fully distributed ECC-based key management for mobile ad-hoc networks", *Elsevier Computer Networks*, Volume 113, 11, Pages 269-283, 2016.

[3] T. Shu and M. Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", *IEEE Transactions On Mobile Computing*, Vol. 14, No. 4, April 2015.

[4] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks", *In Computer Communication*, vol. 30, nos. 11/12, pp. 2314-2341, Sept. 2007.

[5] H.-Smith, J. Wetherall, A. Adekunle, "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks", *IEEE Transactions on Mobile Computing*, Volume: PP, Issue: 99, Jan-2017.

[6] ChEn Xi, Sun Liang, MA JianFeng, MA Zhuo, "A Trust Management Scheme Based on Behaviour Feedback for Opportunistic Networks", *Network Technology And Application, China Communications*, April 2015.

[7] Ming Li, Sergio Salinas, Pan Li, J. Sun, and X. Huang, "MAC-Layer Selfish Misbehaviour in IEEE 802.11 Ad Hoc Networks: Detection and Defence", *IEEE Transactions On Mobile Computing*, Vol. 14, No. 6, June 2015.

[8] S. K. Dhurandher, et al., "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems", *IEEE System Journal*, Vol. 5, No. 2, 2011.

[9] E. M. Shakshuki, N. Kang, and T. R. Sheltami, "EAACK-A Secure Intrusion-Detection System for MANETs", *IEEE Transactions On Industrial Electronics*, Vol. 60, No. 3, March 2013.

[10] R. Lacuesta, J. Lloret, M. Garcia, and L. Penalver, "A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation", *IEEE Transactions On Parallel And Distributed Systems*, Vol. 24, No. 4, April 2013.

[11] C. E. Perkins, E. M. Royer, and S. R. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing", *IETF INTERNET-DRAFT, MANET working group*, Feb. 2003.

[12] R. V. Boppana and Xu Su, "On the Effectiveness of Monitoring for Intrusion Detection in Mobile Ad Hoc Networks", *IEEE Transactions On Mobile Computing*, Vol. 10, No. 8, August 2011.

[13] M. G. Zapata and N. Asokan, "Securing Ad hoc Routing Protocols", *In Proceedings of the 1st ACM workshop on Wireless security*, Atlanta, GA, USA, pp. 1-10, 2002.

[14] J. Yan, J. Ma, F. Li, and S.J. Moon, "Key Pre-distribution Scheme with Node Revocation for Wireless Sensor Networks", *In Ad Hoc and Sensor Wireless Networks*, vol. 10, nos. 2/3, pp. 235-251, 2010.

[15] S. Sen, J. A. Clark, J. E. Tapiador, "Security threats in mobile Ad hoc networks", *In Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, Florida: Taylor & Francis, pp. 127-146, 2010.

[16] I. Khalil and S. Bagchi, "Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure", *IEEE Transactions On Mobile Computing*, Vol. 10, No. 8, August 2011.

[17] S. Jain, Shastri A, Chaurasia BK, "Analysis and Feasibility of Reactive Routing Protocols with Malicious Nodes in MANETs", *In Proceeding International Conference on Communication Systems and Network Technologies*, 2013.

[18] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs", *IEEE Trans. Mobile Computing*, vol. 6, no. 5, pp. 536-550, May 2007.

[19] R. A. Shaikh, H. Jameel, B. J. d Auriol, H. Lee, S. Lee, and Y.-J. Song, "Group-based trust management scheme for clustered wireless sensor networks", *IEEE Trans. Parallel Distributed System*, Vol. 20, pp. 1698-1712, Nov. 2009.

[20] Chen, S. Garg, and K. S. Trivedi, "Network Survivability Performance Evaluation: A Quantitative Approach with Applications in Wireless Ad-hoc Networks", *Proc. ACM Int'l Workshop Modelling, Analysis, and Simulation of Wireless and Mobile Systems*, pp. 61-68, Sept. 2002.

[21] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions", *IEEE Wireless Communication*, vol. 11, no. 1, pp. 38-47, Feb. 2004.

[22] Abedi O, M. Fathy, "Enhancing AODV routing protocol using mobility parameters in VANET", *IEEE/ACS International Conference on Computer Systems and Applications*, AICCSA 2008.

[23] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: A Lightweight Hop-by-Hop Authentication Protocol For Ad-Hoc Networks", *In Ad Hoc Networks Journal*, vol. 4, no. 5, pp. 567-585, Sept. 2006.

[24] Zhang, Y. Song, Y. Fang, and Y. Zhang, "On the price of a security in large-scale wireless ad hoc networks", *IEEE/ACM Transaction Network.*, vol. 19, no. 2, pp. 319-332, Apr. 2011.

[25] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", *Proc. 8th Ann. Int'l Conf. Mobile Computing and Networking (MobiCom 2002), ACM Press*, pp. 12-23, 2002.

[26] A. P. Gopi, E. S. Babu, C. N. Raju, S. A. Kumar, "Designing an Adversarial Model Against Reactive and Proactive Routing Protocols in MANETS: A Comparative Performance Study", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol 5 No 5, 2015.
[27] S. Ashok Kumar, E. Suresh Babu, C. Nagaraju, A. Peda Gopi, "An Empirical Critique of On-Demand Routing Protocols against Rushing Attack in MANET", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol 5 No 5, 2015.
[28] V. Hagawane, A. A. Shrivastav, K. Tambekar, "Reorganization of intruder Using Ad-Hoc Network And RFID", *IAES International Journal of Robotics and Automation (IJRA)*, Vol 3 No 4, pages 268-271, 2014.

BIOGRAPHIES OF AUTHORS

K. Ramesh Rao , Obtained his M.Tech degree from JNTUA University, Anantapuramu (AP)-India in the field of Computer Science & Engineering. He is a Ph.D Research Scholor at Faculty of Computer Science & Engineering. His main area of interests are Computer Networks, Network Security and Communication Networks.

Dr. S.N. Tirumala Rao, M.Tech ., Ph.D . He is working as Professor and Head of the Department of CSE, NarasaraoPeta Engineering College, Narasaraopet, Guntur(AP)-India. His Areas of research are Data Mining, Multi-Core and Parallel Programming and Computer Networks. He Published more than 20 National and International Journals and organized several National and International Conferences.Books Published: Advanced Unix Programming HI-Tech Publisher

Prof. P.Chenna Reddy, B.Tech, MS., M.Tech, Ph.D . He is Professor of CSE Department and Director Academic Audit, Jawaharlal Nehru Technological University Anantapur, Anantapuramu(AP)-India. He Published more than 60 National and International Journals and participated in more than 30 National and International Conferences. His Research areas are Computer Networks, Bio-inspired Networking, Image Processing, Teaching Methodology. His area of Interest is Computer Networks.